



Mapping ISO 27001:2013 and COBIT 2019 Framework to STRIDE Threat Modeling Using Qualitative Descriptive Research

Hermawan Setiawan^{1*}, Nisrina Aliya Hana¹, Rayhan Ramdhany Hanaputra¹

¹Crypto Software Engineering, Politeknik Siber dan Sandi Negara, Indonesia

Correspondence: E-mail: hermawan.setiawan@poltekssn.ac.id

ABSTRACT

Information is a fundamental asset in every organization. The protection of this asset, through information security processes, is critical. COBIT and ISO27001 are reference frameworks for information security management that help organizations assess their security risks and implement appropriate security controls. One of the most important parts of IT in the COBIT framework is information security management which includes confidentiality, integrity, and availability of resources. Since the issues addressed in COBIT information security management are areas covered by the ISO/IEC27001 standard, the best option to address information security management in a COBIT infrastructure is to use the ISO/IEC27001 standard. For the existence and complementary use of COBIT and ISO27001, mapping COBIT processes to ISO/IEC 27001 controls is very useful. This paper explores the role of information security in COBIT and describes the approach of mapping COBIT processes to ISO/IEC27001 controls for information security management.

ARTICLE INFO

Article History:

Submitted/Received 05 Aug 2024

First Revised 09 Sep 2024

Accepted 01 Oct 2024

First Available online 31 Oct 2024

Publication Date 31 Oct 2024

Keyword:

Information security
management,
COBIT,
ISO/IEC 27001,
PDCA cycle,
STRIDE.

1. INTRODUCTION

In the era of globalization, information security and information technology (IT) governance have become critical factors in determining the operational success of an organization. Along with the increasing dependence on technology, the risks related to information security and IT management are also increasingly complex and diverse. Organizations are faced with the challenge of managing and protecting their information assets from various threats, both internal and external.

Based on a report from Badan Siber dan Sandi Negara (BSSN), it was recorded that the number of cyber-attack cases in Indonesia from the beginning of 2020 to April 12, 2020 was 88 million. From this number, 56% were identified as cases of trojan-activity attacks, 43% were cases of information-gathering attempts, and 1% were cases of web application attacks [1]. Meanwhile, the results of monitoring the total number of cyber-attack cases in Indonesia at the end of 2020 reached 495 million with the most attacks being trojan activity and data theft [2]. This shows that there has been an increase in cyber-attacks in Indonesia by 205 million when compared to the number of cyber-attack cases in 2019 which was 290 million cases [3].

Implementation of information security is an important thing for an organization to do. Information security is defined as the protection of information from creation to disposal of data, through logical, technical, physical, and organizational steps that prevent the loss of confidentiality, integrity, and availability of information [4]. This information security needs to be implemented to ensure specific security so that the objectives of a company or organization can be met [5]. According to a survey conducted in the United Kingdom (UK), it is known that 74% of the technology industry sector its research results revealed that high technology security is one of the most crucial things in their organization's senior management [6].

Cybersecurity is part of information security that protects information assets from threats to information processed, stored, and transmitted by interconnected information systems [7]. To improve information security within an organization, special controls need to be carried out to measure the level of cybersecurity that has been implemented. https://drive.google.com/drive/folders/1nh_raMhoknQlt-YzzRVmc5m-SYRJFVazbe used to audit/measure the level of cybersecurity, including COBIT and ISO 27001 [8]. However, although there are various standards, the unique needs of each organization limit the use of the types of frameworks available [1].

An effective IT governance and information security management framework is essential to help organizations achieve their strategic objectives while ensuring the security and integrity of data. Two of the most well-known and widely used frameworks in this area are COBIT (Control Objectives for Information and Related Technologies) and ISO/IEC 27001. While both aim to improve information governance and security, their approaches and focus differ significantly.

COBIT, developed by ISACA, is a framework that provides comprehensive guidance on IT governance and management. COBIT provides a structure that enables organizations to achieve their business objectives through effective IT management. The framework covers various aspects of IT, including risk management, internal control, and regulatory compliance. COBIT is designed to help organizations ensure that IT supports and enhances their business strategy.

ISO/IEC 27001, on the other hand, is an international standard that specifies requirements for an information security management system (ISMS). This standard is designed to help

organizations manage and protect their information through the systematic and structured implementation of policies and procedures. ISO/IEC 27001 emphasizes the importance of risk management and ongoing information protection, ensuring that organizations can address and mitigate the impact of information security threats.

Although both frameworks share the same ultimate goal of improving information security and governance, their approaches differ. COBIT focuses more on the overall governance of IT, including how IT can support the achievement of business objectives and the management of IT risks in general. Meanwhile, ISO/IEC 27001 focuses on managing information security through the implementation of an internationally recognized ISMS.

Organizations are often faced with the dilemma of choosing the most appropriate framework for their needs. Understanding the differences, advantages, and disadvantages of each framework is an important step in making the right decision. This study aims to provide a comparative analysis between COBIT and ISO/IEC 27001.

2. METHODS

In this study, a comparison and mapping of features in the cybersecurity framework based on existing literature studies with descriptive methods will be conducted, where the object of research is in the form of literature. The literature in question is in the form of scientific journals, books, articles in the mass media, and statistical data [9]. This study presents a comparison and mapping of two standards for measuring information security, namely COBIT and ISO 27001. Each standard has advantages and disadvantages. The analysis was carried out using qualitative analysis based on the STRIDE threat model.

3. BASIC CONCEPT

3.1. COBIT Framework

Control Objectives for Information and Related Technology (COBIT) is a set of best practices for information technology governance created by the Information Systems Audit and Control Association (ISACA), and the IT Governance Institute (ITGI) [10].

COBIT provides IT managers, auditors, and users with a set of generally accepted measures, indicators, processes, and best practices to assist them in maximizing the benefits gained through the use of information technology and developing appropriate IT governance and control within an enterprise. COBIT's mission is to help managers, auditors, and users understand their IT systems and decide on the level of security and control needed to protect their enterprise assets through the development of an IT governance model [10]. COBIT can be applied broadly for a variety of purposes. COBIT covers security in addition to all other risks that can occur with the use of IT.

Enterprise governance (the systems used to manage and control an organization) and IT governance (the systems used to manage and control an organization's IT) are closely related from a COBIT perspective. Enterprise governance is inadequate without IT governance and vice versa. IT can extend and influence an organization's performance, but it must be subject to adequate governance. On the other hand, business processes require information from IT processes, and this interdependence must also be managed [11].

The purpose of the COBIT framework is to provide management with an IT governance model that helps them control and manage information and related technology. The framework describes how IT processes deliver the information the business needs to achieve its objectives. This delivery is driven through 34 high-level control objectives, one for each IT process, contained in four domains. This framework identifies information criteria (effectiveness, efficiency, confidentiality, integrity, availability, compliance, and reliability), as well as IT resources (people, applications, technology, facilities, and data) that are critical for

IT processes to fully support business objectives. The IT Governance Institute has identified four domains as the building blocks of the COBIT framework, as illustrated in **Figure 1** [12]. This structure is based on the PDCA cycle.

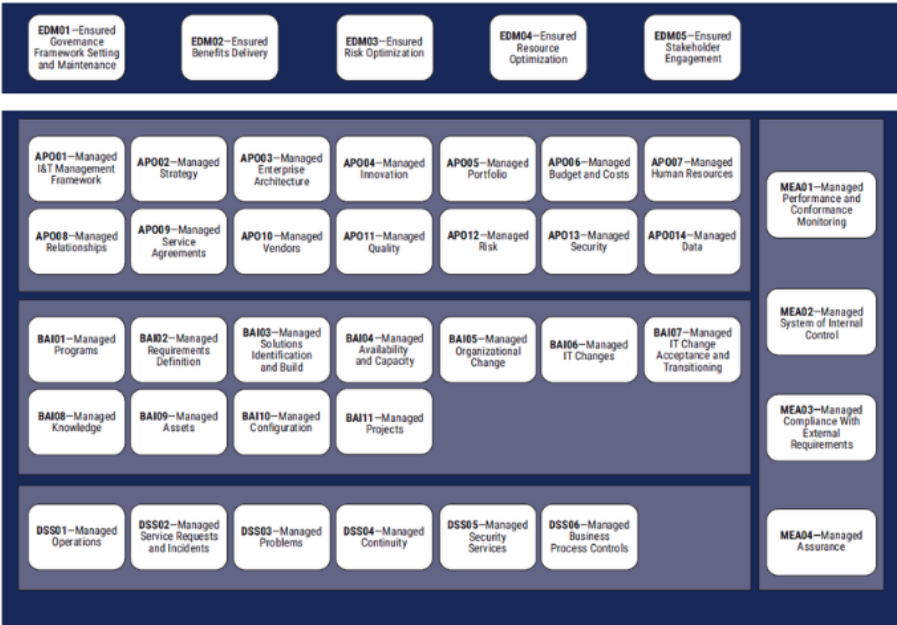


Figure 1. COBIT Domain

Effective information security requires an integrated set of security, management, and governance processes to plan, organize, and address an organization’s information security risks. COBIT provides an integrated governance, management, and process framework for implementing and executing information security. COBIT describes sound processes, practices, and control objectives for managing and operating IT systems, including their security status. Organizations using this framework report an improved ability to deliver high-quality services to their customers, including the ability to measure and meet confidentiality, availability, and integrity requirements. COBIT supports the need for security to be addressed as part of every business function. Although only one COBIT process (DS5) is specifically dedicated to security, the control objectives related to security are spread across processes in each domain. The COBIT security baseline document [13] highlights the high-level COBIT control objectives related to information security across the four domains in the COBIT framework.

3.2 ISO/IEC 27001 Framework

ISO/IEC 27001 originated from a code of good practice published by the UK Department of Trade and Industry in 1989, which later evolved into BS7799 [14]. ISO/IEC 27001 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving a documented Information Security Management System (ISMS) in the context of the organization's overall business risks. ISO/IEC 27001 specifies requirements for the implementation of security controls tailored to the needs of the organization or part of it. The ISMS is designed to ensure the selection of adequate and proportionate security controls that protect information assets and provide confidence to interested parties. The proposed requirements are structured in an 11-clause classification covering 39 objectives driven by 133 controls [15][16].

ISO/IEC 27001 specifies how an organization should address the confidentiality, integrity, and availability requirements of its information assets and integrate these into its Information

Security Management System (ISMS) [17][19]. This standard is used worldwide by organizations, both commercial and governmental, as a basis for the management of organizational policies and the implementation of information security. It is used by small, medium, and large organizations in a variety of business sectors. It is designed to be flexible enough to be used by all types of organizations. It has become the de facto “common language” for information security management [15][16].

The standard introduces a cyclical model known as the “Plan-Do-Check-Act” (PDCA) model that aims to establish, implement, monitor, and improve the effectiveness of an organization’s ISMS. The PDCA cycle has the following four phases as shown in **Figure 2**.

- Plan – establish the ISMS: Establish relevant ISMS policies, objectives, processes, and procedures to manage risk and improve information security to produce outcomes consistent with the organization’s overall policies and objectives [10].
- Do – implement and operate the ISMS: Implement and operate the ISMS policies, controls, processes, and procedures [18].
- Check – monitor and review the ISMS: Assess and, where applicable, measure process performance against the ISMS policies, objectives, and practical experience and report the results to management for review [20].
- Act – maintain and improve the ISMS: Take corrective and preventive actions, based on the results of ISMS internal audits and management reviews or other relevant information, to achieve continual improvement of the ISMS [4].

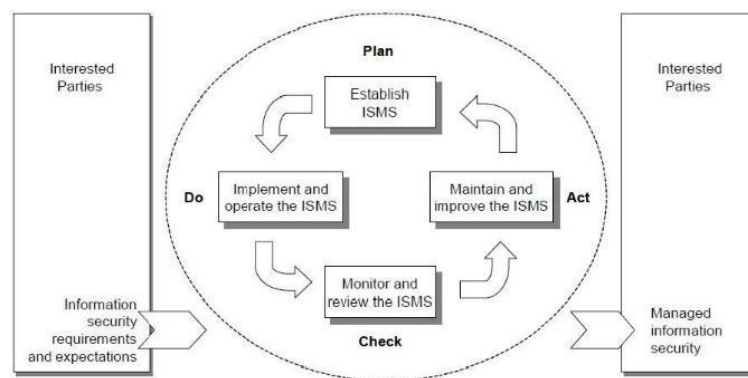


Figure 2. PDCA Model in ISMS Process

Table 1 below serves as a comprehensive overview of the key components necessary for establishing, implementing, maintaining, and continually improving an information security management system (ISMS) in alignment with ISO/IEC 27001.

Table 1. ISO/IEC 27001 Control Objectives.

Controls	Control Objectives
A.5 Security policy	A.5.1 Information security policy
A.6 Organizational information security	A.6.1
A.6.2	External parties
A.7 Asset Management	A.7.1
A.6.3	Information classification
A.8 Human resources security	A.8.1
A.8.2	During employment
A.6.4	Termination or change of employment
A.9 Physical and environmental security	A.9.1
A.6.5	Equipment security

3.3 STRIDE

STRIDE is a threat modelling method used in security analysis to identify and categorize different types of security threats. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege [21]. This methodology helps in systematically analyzing potential threats across a wide range of systems, including cyber-physical systems, automotive security, distributed control systems, software-defined network applications, and computer network security [21]. The STRIDE model helps in detecting and preventing threats by guiding Spoofing (a threat to authentication where an unauthorized entity pretends to be a legitimate entity), Tampering (a threat to integrity where data or systems are altered unauthorizedly), Repudiation (a threat to accountability where an entity can deny actions that have been taken), Information Disclosure (a threat to confidentiality where information is leaked to unauthorized parties), Denial of Service (a threat to availability where a service or system becomes unavailable to authorized users), and Elevation of Privilege (a threat to authorization where an entity is granted higher access rights than it should be). The explanation can also be seen in **Figure 3**.

STRIDE-LM	Threat	Property	Definition	Controls
S	Spoofing	Authentication	Impersonating someone or something	Authentication Stores, Strong Authentication mechanisms
T	Tampering	Integrity / Access Controls	Modifying data or code	Crypto Hash, Digital watermark/ isolation and access checks
R	Repudiation	Non-repudiation	Claiming to have not performed a specific action	Logging infrastructure, full-packet-capture
I	Information Disclosure	Confidentiality	Exposing information or data to unauthorized individuals or roles	Encryption or Isolation
D	Denial of Service	Availability	Deny or degrade service	Redundancy, failover, QoS, Bandwidth throttle
E	Elevation of Privilege	Authorization / Least Privilege	Gain capabilities without proper authorization	RBAC, DACL, MAC; Sudo, UAC, Privileged account protections

Figure 3. Figure of Explanation STRIDE Threat Model

4. RESULTS AND DISCUSSION

The fundamental difference between COBIT and ISO 27001 is that ISO 27001 focuses only on information security, while COBIT focuses on more general information technology controls. As such, COBIT has a broader scope of general information technology topics but does not have the detailed information security requirements of ISO 27001. If an organization were to address all of the security controls in ISO 27001, then they would cover most of COBIT in the process—especially the DS5 section that ensures system security. However, COBIT covers a much larger set of issues related to information technology governance and is typically used as part of an overall corporate governance framework. One of the most important areas of information technology in the COBIT framework is information security management, which covers the confidentiality, integrity, and availability of resources. Since the issues raised are areas covered by the ISO/IEC 27001 standard, and this standard also considers the PDCA cycle as an infrastructure, the best option to fulfill information security management in the COBIT infrastructure is to use the ISO/IEC 27001 standard. For the coexistence and complementary use of COBIT and ISO/IEC 27001, a mapping between COBIT and ISO/IEC 27001 is very useful.

The purpose of the mapping is to provide an integrated way for the complementary use of COBIT and ISO/IEC 27001 in information security management. Mapping ISO/IEC 27001 to COBIT processes allows organizations to reduce the overall cost of maintaining an acceptable level of security, manage risks effectively, and reduce the overall level of risk.

For the mapping between these frameworks, each COBIT process is examined, and the corresponding ISO 27001 Annex A control objectives are indicated. Based on the ISO/IEC 27001:2005 domains and COBIT processes, the relationship between the subjects and control parameters of both standards is given in **Table 2**.

Table 2. Mapping of ISO/IEC 27001 and COBIT to STRIDE Threat Model.

No	ISO/IEC 27001	COBIT 2019	STRIDE Threat Model
1	Management direction for information security	EDM (Evaluate, Direct, and Monitor)	I - Information Disclosure
2	Internal organization	EDM	I - Information Disclosure
3	Mobile devices and teleworking	EDM	T - Tampering
4	Before employment	APO 07 (Manage Human Resources)	S - Spoofing
5	During employment	APO 07	S - Spoofing
6	Termination and change of employment	APO 07	S - Spoofing
7	Responsibility for assets	BAI 09 (Manage Assets)	I - Information Disclosure
8	Information classification	BAI 09	I - Information Disclosure
9	Media handling	BAI 09	T - Tampering
10	Business requirements of access control	DSS 05 (Manage Security)	T - Tampering
11	User access management	DSS 05	S - Spoofing
12	User Responsibilities	DSS 05	S - Spoofing
13	System and application access control	DSS 05	T - Tampering
14	Cryptographic controls	DSS 05	I - Information Disclosure, T - Tampering
15	Secure areas	DSS 05	T - Tampering
16	Equipment	DSS 05	T - Tampering
17	Operational procedures and responsibilities	DSS 01 (Manage Operations)	T - Tampering
18	Protection from malware	DSS 05	I - Information Disclosure, T - Tampering
19	Backup	APO 14 (Manage Availability)	T - Tampering
20	Logging and monitoring	DSS 05	S - Spoofing, T - Tampering
21	Control of operational software	DSS 05	T - Tampering
22	Technical vulnerability management	DSS 05	I - Information Disclosure, T - Tampering
23	Information systems audit considerations	MEA 04 (Monitor, Evaluate, and Assess)	S - Spoofing
24	Network security management	DSS 05	T - Tampering

25	Information transfer	DSS 05	I - Information Disclosure
26	Security requirements of information systems	APO 13 (Manage Security)	S - Spoofing
27	Security in development and support processes	APO 04 (Manage Development)	S - Spoofing, T - Tampering
28	Test data	APO 14	T - Tampering
29	Information security in supplier relationships	APO 10 (Manage Supplier Relationships)	S - Spoofing
30	Supplier service delivery management	APO 10	S - Spoofing
31	Management of information security incidents and improvements	DSS 05	I - Information Disclosure, T - Tampering
32	Information security continuity	DSS 04 (Manage Continuity)	T - Tampering
33	Redundancies	DSS 04	T - Tampering
34	Compliance with legal and contractual requirements	MEA 03 (Monitor, Evaluate, and Assess Compliance)	S - Spoofing
35	Information security reviews	APO 13	S - Spoofing

The following **Table 3** provides a detailed overview of these mappings, highlighting the alignment between the standards and the threat model to enhance organizational security posture.

Table 3. Scenario Example of Threat

No	Scenario	Threat	ISO/IEC 27001	COBIT 2019	STRIDE
1	Data Theft through Unauthorized Access	Spoofing (S)	11. User Access Management	DSS 05 (Manage Security)	S – Spoofing
2	Malware Attack on the System	Tampering (T)	18. Protection from Malware	DSS 05 (Manage Security)	I - Information Disclosure, T – Tampering
3	Non-compliance with regulations	Spoofing (S)	34. Compliance with Legal and Contractual Requirements	MEA 03 (Monitor, Evaluate, and Assess Compliance)	S – Spoofing

In scenario 1, attackers gain unauthorized access to a system due to inadequate access controls. This poses a significant risk of data theft. By mapping the ISO/IEC 27001 standard, specifically the user access management controls, and the COBIT 2019 framework, particularly the DSS 05 domain focused on security management, organizations can implement stricter access controls and user management protocols. This reduces the risk of data theft through unauthorized access, ensuring that only authorized individuals have access to sensitive information.

Scenario 2 involves malware infiltrating the system, causing damage, or accessing sensitive information. Such an attack can lead to data tampering and information disclosure. By implementing the controls outlined in ISO/IEC 27001 for malware protection and leveraging the security management practices from COBIT 2019, organizations can enhance

their ability to detect and prevent malware attacks. These measures include robust malware protection strategies and continuous security monitoring, which help safeguard systems from malicious software.

In scenario 3, an organization fails to meet applicable regulatory requirements, which can result in fines or reputational damage. By clearly mapping the requirements of ISO/IEC 27001 and COBIT 2019, organizations can ensure better compliance with legal and contractual obligations. The ISO/IEC 27001 standard emphasizes compliance with regulatory requirements, while COBIT 2019's MEA 03 domain focuses on monitoring, evaluating, and assessing compliance. Together, these frameworks provide a comprehensive approach to maintaining compliance and mitigating the risks associated with regulatory non-compliance.

5. CONCLUSION

Information security plays a critical role in protecting an organization's assets. Since no single formula can guarantee 100% security, a set of benchmarks or standards is needed to help ensure that adequate levels of security are achieved, resources are used efficiently, and best security practices are adopted. Systems such as COBIT and ISO/IEC 27001 can be used together as a foundation for developing a solid information security process. For the coexistence and complementary use of COBIT and ISO/IEC 27001 as a reference framework for information security management, mapping COBIT processes to ISO/IEC 27001 control objectives can be used. In this paper, we describe the mapping between COBIT and ISO/IEC 27001. Mapping ISO/IEC 27001 to COBIT processes enables organizations to reduce the overall cost of maintaining acceptable levels of security, manage risks effectively, and reduce the overall level of risk. In addition, the use of this mapping will also reduce confusion and dissonance that exists between IT and Audit. For future work, we plan to design a comprehensive and cost-effective framework for organizational use in balancing the implementation of ISO/IEC 27001 and COBIT processes.

6. AUTHORS' NOTE

The authors declare that there is no conflict of interest regarding the publication of this article. The authors confirmed that the paper was free of plagiarism.

7. REFERENCES

- [1] E. Handoyo. "Analisis Tingkat Keamanan Informasi: Studi Komparasi Framework Cobit 5 Subdomain Manage Security Services (DSS05) dan NIST Sp 800 – 55," *J. CoSciTech Computer Sci. Inf. Technol.*, vol. 1, no. 2, pp. 76–83, Oct. 2020. doi: 10.37859/coscitech.v1i2.2199.
- [2] "Rekap Serangan Siber (Januari - April 2020)," *BSSN*, Online. Available: <https://www.bssn.go.id>.
- [3] "BSSN: Malware Trojan Dominasi Serangan Siber di 2020," *Tempo.co*, Online. Available: <https://www.tempo.co/>.
- [4] "Laporan Tahunan 2019 PUSOPSKAMSINAS," *BSSN*, Online. Available: <https://www.bssn.go.id>.
- [5] A. Ključnikov, L. Mura, and D. Sklenár, "Information Security Management in SMEs: Factors of Success," *Entrep. Sustain. Issues*, vol. 6, no. 4, pp. 2081–2094, Jun. 2019. doi: 10.9770/jesi.2019.6.4(37).
- [6] Department for Digital Culture Media and Sport, "Reino Unido Cyber Security 2018," *Cyber Security. Breaches Surv.*, no. 1, pp. 1–58, 2018.

- [7] M. G. Cains, L. Flora, D. Taber, Z. King, and D. S. Henshel, "Defining Cyber Security and Cyber Security Risk within a Multidisciplinary Context using Expert Elicitation," *Risk Anal.*, Vol. 42, No.8, pp. 1643-1649. Feb. 2021. doi: <https://doi.org/10.1111/risa.13687>.
- [8] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology using nist csf, cobit, iso/iec 27002 and pci dss" *Int. J. Informatics Vis.*, vol. 4, no. 4, pp. 225–230, Jul. 2020. DOI: 10.30630/joiv.4.4.482.
- [9] D. Prasanti, D. R. Fitriani, "Penelitian Kepustakaan (Library Research) dalam Penelitian Pendidikan IPA," *Pembentukan Anak Usia Dini Keluarga, Sekolah, Dan Komunitas*, vol. 2, no. 1, p. 15, jun. 2018. DOI: 10.31004/obsesi.v2i1.2
- [10] Etzler, J. (2008). IT Governance According to COBIT (Master's Thesis). Royal Institute of Technology, Stockholm, Sweden. OAI: <https://api.core.ac.uk/oai/oai:CiteSeerX.psu:10.1.1.66.2955>
- [11] IT Governance Institute (ITGI). (2000). *COBIT Mapping: Mapping of ISO/IEC 17799:2000 with COBIT*, 2nd Edition, Printed in the United States of America, United States of America.
- [12] R. Witjaksono. "Audit Sistem Informasi Akademik Universitas Telkom Menggunakan Framework COBIT 5 Domain DSS Untuk Optimasi Proses Service Delivery," *Jurnal Rekayasa Sistem & Industri (JRSI)*, 6(01), 16-23. Jun. 2019. doi: 10.25124/jrsi.v6i1.341
- [13] IT Governance Institute (ITGI), "COBIT Security Baseline. An Information Security Survival Kit", Rolling Meadows: Author. Retrieved (2008) Jun. 30, from <http://www.isaca.org>.
- [14] A. A. Alrehili and O. H. Alhazmi, "ISO/IEC 27001 standard: Analytical and Comparative Overview," in *Proc. Int. Conf. Adv. Data-driven Comput. Intell. Syst.*, Sep. 2023, pp. 143–156. doi: 10.1007/978-981-99-9524-0_12.
- [15] M. Stamp, *Information Security: Principles and Practice*. Hoboken, NJ, USA: Wiley, 2011.
- [16] T. R. Peltier, *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. Boca Raton, FL, USA: CRC Press, Apr. 2016.
- [17] K. L. Thomson and R. V. Solms, "Information Security Obedience: a Definition", *J Computers & Security*, Vol. 24, pp. 69-75, Feb 2005. doi: 10.1016/j.cose.2004.10.005.
- [18] T. Humphreys. *Guide to the Implementation and Auditing of ISMS Controls Based on ISO/IEC 27001*, BSI British Standards Institution, 2005.
- [19] Ganji D, Kalloniatis C, Mouratidis H, Gheytaasi SM. Approaches to Develop and Implement iso/iec 27001 Standard-Information Security Management Systems: A Systematic Literature Review. Vol.12, No.3, pp. 228-238, *Int. J. Adv. Softw.* 2019.
- [20] Haufe, Knut, et al. "A Process Framework for Information Security Management." *International Journal of Information Systems and Project Management*, Vol. 4, No.4, pp. 27-47. Aug. 2016. doi: 10.12821/ijispm040402
- [21] H. Kayan, M. Nunes, O. Rana, P. Burnap, C. Perera. "Cybersecurity of Industrial Cyber-Physical Systems: A review". *ACM Computing Surveys (CSUR)*. Vol.54, No.11, pp. 1-35 Sep. 2022. doi: <https://doi.org/10.1145/3510410>